GDPR – Privacy Policy

Statement of Intent

Ripponden Preschool is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). We may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, Department for Education, other schools and educational bodies, children's services and other third parties, such as payroll providers or cashless till services.

This policy is in place to ensure all staff and committee members are aware of their responsibilities and outlines how the preschool complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and Ripponden Preschool believes that it is good practice to keep clear practical policies, backed up by written procedures. This policy complies with the requirements set out in the GDPR

Applicable Data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual. The GDPR applies to both electronic personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data.

Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Data will not be kept for any longer than is necessary in accordance with EYFS and Ofsted legislation. *(See retention policy.)*
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

Accountability

Ripponden Pre School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. We will provide comprehensive, clear and transparent privacy policies. Records of data collections will be managed or monitored on a data register.

Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:— Compliance with a legal obligation. — For the performance of a contract with the data subject or to take steps to enter into a contract. — Protecting the vital interests of a data subject or another person. — For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the Data Protection Act (DPA) will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.
- Where a child is under the age of 16 or younger if the law provides it (up to the age of 13), the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

The Right to be Informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, and easily accessible.

- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- The retention period of data.
- The existence of the data subject's rights, including the right to: — Withdraw consent at any time. — Lodge a complaint with a supervisory authority.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

The Right of Access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The manager will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training. Staff must report any data breach or potential breach as soon as possible to the Data Protection Officer or a member of the Senior Management Team.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects
- Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

Data Security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is kept in a locked and secure location.

Access to the school's network is controlled and access to sensitive and confidential data on the network is restricted to only those members of staff who require the information to perform their duties effectively.

Electronic devices are kept securely when not in use, e.g. in a locked cabinet.

Devices holding pupil and staff photos will be regularly wiped to delete all images.

Memory cards will be kept in a locked cabinet when not in use and will be wiped regularly.

Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

No personal data or sensitive personal data must be shared by text or on social media

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices or paperwork under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data,

All staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- The person or organisation who will receive the data has been outlined in a privacy notice.
- The person or organisation who will receive the data has confirmed in writing that they comply with the GDPR and any other relevant data protection legislation.

Under no circumstances are volunteers, visitors or unauthorised third parties allowed access to confidential or personal information. Those visiting areas of the school containing sensitive information (Learning journeys) are supervised at all times. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Photography

The school understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

The school will always indicate its intentions for taking photographs of pupils and will obtain permission before publishing them.

If the school wishes to use images of pupils in a publication, such as the school website, prospectus, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR

Data Retention and Storing Pupil Data

Data will not be kept for longer than is necessary. The school follows the Information Commissioner's guidance on retention of documents, including the Information and records Management Society's Retention Guidelines for School.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

DBS Data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

GDPR Guidance:

Article 3 - the best interests of the child must be a top priority in all decisions and actions that affect children
Article 16 – the right to privacy
Article 36 – Governments must protect children from all forms of exploitation.

Also see (Retention Policy)

This policy was adopted on 25 May 2018.

Reviewed September 2019 Signed ..... Manager